Home Office

Early Engagement Notice for:

C23801 Software Defined-WAN Services

sourced either from (RM1557.13) G-Cloud or from (RM3808) Network Services 2.

First published: 2023-02-23

Re-published with more developed requirement: 2023-04-04

PURPOSE OF NOTICE:

This notice is for suppliers on both the Crown Commercial Services (CSS) Frameworks **G-Cloud 13 (RM1557.13)** and **Network Services 2 (RM3808), Lot 1**, only. This notice is part of early market engagement to support the Home Office objective of sourcing a single call-off contract, delivered by one supplier, as a single Direct Award against one of these two frameworks.

The aim is to procure a contract that provides continuity of network encryption services protecting police and law enforcement community network communications from criminal, hostile state or terrorist penetration.

The driver for this opportunity is the expiry in October 2024 of a G-Cloud 11 contract with Fujitsu for a Cisco-based Software-Defined Wide Area Network (SD-WAN) service, awarded in 2020.

EXCLUSIONS:

Replacement of the law enforcement community's network connectivity.

LIMITATIONS:

The Home Office reserves the right not to proceed with any procurement described in this notice; the right to revise the approach and timelines; the right to withdraw or revise this notice and other information issued to the market, all without obligation.

The Home Office will not contribute in any way to meeting production costs of any response to this notice.

INDICATIVE TIMELINE:

1. **FEB-JUNE 2023:** Market engagement through clarification questions, Request(s) for Information and updates to this notice; in parallel with refinement of requirements and visits to reference sites
2. **JULY 2023:** Evaluation of offerings on CCS catalogues for RM1577.13 and for RM3808, Lot 1
3. **AUG 2023:** Direct Award of one contract
4. **SEPT 2023:** Mobilisation of successful supplier
5. **OCT 2024:** End of transition (ie 13 month transition window)

SOLUTION DELIVERY:

The selected supplier will deliver the continuity solution into the Law Enforcement Community Network (LECN) programme. The LECN programme is progressing a Business Case to spend a 7-figure (GBP) budget on the contract over a minimum three-year period from calendar year 2023.

BUSINESS ENGAGEMENT:

The LECN programme's main engagement with the autonomous and diverse law enforcement community takes place through a Business User Group (BUG). Representatives on the BUG include policing, other law enforcement agencies, National Police Technology Council (NPTC), other government departments, Arms-Length Bodies, incumbent suppliers to law enforcement agencies, and Home Office product owners of national policing applications.

RISK APPETITE:

All data is OFFICIAL.

The Home Office expects to consult Police and National security authorities when considering the suitability of solutions, given the sensitivity of network communication across the law enforcement community.

The LECN Programme has a low appetite for solution development because of the risk to continuity and the risk of business disruption. The expectation is

that the Home Office will buy a verifiable Cisco-based SD-WAN solution already being delivered in a secure context.

SCALE / GEOGRAPHY:

Nearly 100 law enforcement organisations (policing and suppliers) and approximately 50 other government departments / Arms-Length Bodies are in scope for receipt of contract services. These organisations operate from about 160 sites within the UK and offshore. All data-centres are in the UK.

CONSTRAINTS:

Transition to the SD-WAN solution should complete by October 2024 (twenty twenty-four).

EXISTING ARRANGEMENTS:

Fujitsu provides a Cisco-based SD-WAN service: https://www.digitalmarketplace.service.gov.uk/g-cloud/services/319976427300466

REQUIREMENTS SCOPE:

This requirements statement illustrate what may be key areas for the LECN programme's exam`ination of service providers' published offerings on applicable CCS catalogues. It is not a comprehensive statement and it is subject to development. Requirement scope used in procurement may differ from what is indicated here.

REQ_ID	Topic	Requirement
CP_1_0_001	Functionality	The service's edge devices are controlled centrally by a Cisco SD-WAN orchestrator that automates the application of edge device configuration and application traffic policies.
CP_1_0_002	Functionality	The service provides both physical and virtual Cisco SD-WAN Catalyst 8000 edge devices capable of processing raw data presented at a rate of at least 1Gb/s, while applying traffic steering and FIPS 140-2 (minimum level 2) encryption / decryption assured through National Cyber Security Centre guidance.
CP_1_0_003	Functionality	The service includes a pre-production environment aligned to the production environment where the service provider tests all patches and all software releases

REQ_ID	Topic	Requirement
		before deployment to the production environment.
CP_1_0_004	Functionality	The control plane runs on PSN Assured underlay.
CP_1_0_005	Functionality	The service provider can connect the service to Amazon Web Services and Azure Cloud Platforms.
CP_1_0_006	Functionality	The service enables the buyer to pin traffic to a specified underlay transport mechanism.
CP_1_0_007	Security	The service provider has beneficial ownership within the UK and has a policy of informing the buyer promptly of any anticipated changes to the service provider's beneficial ownership.
CP_1_0_008	Security	The buyer can ensure that data storage and processing is entirely within the United Kingdom.
CP_1_0_009	Security	The buyer can ensure that the service is provided, supported and managed entirely within the United Kingdom.
CP_1_0_010	Security	The service is within the scope of a certified ISO 27001-, equivalent- or superior standard held by the service provider.
CP_1_0_011	Security	The service provided to the buyer is accessible only to the buyer and is not accessible to any other customer of the service provider.
CP_1_0_012	Security	The service implement levels of privilege and authorisation mechanisms that enforce separation of privileges between different types of account.

REQ_ID	Topic	Requirement
CP_1_0_013	Security	The service provider carries out IT Health Check/penetration testing of the service at least once in any 12 month period.
CP_1_0_014	Security	The service provider is ready to ensure it has adequate numbers of staff with Security Check (SC) obtained through the National Security Vetting process.
CP_1_0_015	Security	The service provider is ready to ensure it has adequate numbers of staff with Non-Police Personnel Vetting (NPPV) achieved through the Management Vetting process.
CP_1_0_016	Security	The service provider is willing to undergo Police Assured Secure Facilities (PASF) audits.
CP_1_0_017	Security	The service provides secure role-based portal access to management information and configuration capabilities by web browser from any end-user site.
CP_1_0_018	Service management	The portal provides real-time data and historic data and reports on network state, network performance and application traffic.
CP_1_0_019	Service management	The service can make available, through a standard interface, event-log data including Security Incident and Event Management (SIEM).
CP_1_0_020	Service management	The service provides the buyer with access to a record which tracks the location and status of each accountable security encrypted (ACCSEC) device throughout its life and into its terminal state.
CP_1_0_021	Service management	The service provides secure destruction of equipment that has been withdrawn from use either by the buyer or by the service provider.

REQ_ID	Topic	Requirement
CP_1_0_022	Business continuity	The service's Orchestration components site failover capability is subject to testing at least once in any six-month period.
CP_1_0_023	Business continuity	The service continues unimpaired for at least seven consecutive calendar days if there is a catastrophic failure in a single data centre.
CP_1_0_024	Security	The buyer may audit the service provider's documentation and processes in respect of: standards certifications (eg ISO270001) that are identified in the service provider's service description, in order to assure scope, timing and compliance of these certifications in relation to the supplier's service.
CP_1_0_025	Service management	Phone support from the service provider's service-desk agents is available for users 24 / 7 / 52 and the supplier is ready to address high-severity incidents 24 / 7 / 52 against a 4-hour resolution target which is the subject of a regularly reported performance indicator.
CP_1_0_026	Service management	The service provider can encrypt operational communication between the service provider and the buyer.
CP_1_0_027	Service management	The service is within the scope of a certified ISO/EIC 20000-, equivalent- or superior standard held by the service provider.
CP_1_0_028	Commercial	The service provides orchestrated physical and virtual edge devices with portal access to management information and configuration capabilities, all of which meet the buyer's pricing requirements and PSN requirements, integrated into an SD-WAN solution and without onerous obligation on the buyer to manage

REQ_ID	Topic	Requirement
		elements of service that are outside the scope of the buyer's requirements.
CP_1_0_029	Commercial	The service provider's catalogue provides a firm price on a per-service or a per-unit basis over a defined time period, for each separately-selectable element of the service.
CP_1_0_030	Commercial	The service provider publishes a SFIA (or similar resource-scheme) rate-card with firm pricing for each of the specialisms as follow (or near equivalents): Strategy & Architecture, Solution development & implementation, Service management, Procurement & management support, Client interface; for each specialism there is firm pricing at one or more SFIA grades between 3 to 5 (or equivalent grades for a similar resource scheme).
CP_1_0_031	Referenceability	The service provider has implemented a service meeting requirements CP_1_0_001, CP_1_0_002 and CP_1_0_003 for at least one other customer and can provide the buyer with related references that the buyer can follow up independently of the service provider.

TO NOTE:

This notice relates to procurement from CCS frameworks with established and unchanging memberships, using Cabinet Office tools which are available to the framework members. There is no supplier registration process.

Procurement will be by compliant Direct Award, based on a review by the LECN programme of service offerings accepted by CCS and published on a relevant CCS catalogue. Please do not send the LECN programme any pricing material or proposals.

At this time we are not providing contact details because, for now, all information about the procurement will be provided as updates to this notice.

NEXT STEPS:

If you believe you have a service (or services) on the relevant CCS Frameworks that may meet the Home Office requirement, you are encouraged to review your service descriptions and to ensure that they are up to date, reflective of your capabilities, and available on the relavant CCS platforms.

You may also want to return to Contracts Finder from time to time, to check for updates to this notice. A suggested search, to obtain the latest version of this notice, is:

https://www.contractsfinder.service.gov.uk/Search with tick-boxes "Early Engagement Notice" "Open" and keywords "LECN" and "C23801".